

UNITED STATES DISTRICT COURT

for the

Western District of Texas

In the Matter of the Seizure of
 (Briefly describe the property to be seized)
 All Funds in JPMorgan Chase Bank Checking
 Account 6801310670 in the names of
 Kevin Pelayo, Edna Pelayo, & Cristine Fredericks

Case No. WZO-117M

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Western District of Texas be seized as being subject to forfeiture to the United States of America. The property is described as follows:

All Funds in JPMorgan Chase Bank Account 6801310670 in the names of Kevin Pelayo, Edna Pelayo, Cristine Fredericks. *Proceeds of violations of Title 18 U.S.C. §§ 371, 641, 1343, & 1956(h) are subject to civil & criminal forfeiture pursuant to Title 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c). Proceeds are subject to civil seizure warrants pursuant to Title 18 U.S.C. § 981(b) and criminal seizure warrants pursuant to Title 21 U.S.C. § 853(f) by Title 18 U.S.C. § 982(b)(1).

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before within 14 days
 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

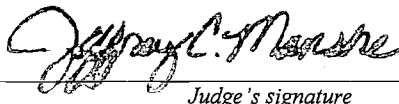
Jeffrey C. Manske, U.S. Magistrate Judge

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 6/9/2020 @ 3:00pm


 Judge's signature

City and state: Waco, TX

Jeffrey C. Manske, U.S. Magistrate Judge

Printed name and title

SEALED

FILED

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

JUN - 9 2020

UNITED STATES DISTRICT COURT

for the

Western District of Texas

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY Ymin
DEPUTY CLERK

In the Matter of the Seizure of)
 (Briefly describe the property to be seized))
 All Funds in JPMorgan Chase Bank Checking) Case No.
 Account 6801310670 in the names of)
 Kevin Pelayo, Edna Pelayo, & Cristine Fredericks)

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Western District of Texas is subject to forfeiture to the United States of America under 18 U.S.C. §

981(a)(1)(C)* (describe the property):

All Funds in JPMorgan Chase Bank Acct 6801310670 in the names of Kevin Pelayo, Edna Pelayo, Cristine Fredericks. *Proceeds of violations of Title 18 U.S.C. §§ 371, 641, 1343, & 1956(h) are subject to civil & criminal forfeiture pursuant to Title 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c). Proceeds are subject to civil seizure warrants pursuant to Title 18 U.S.C. § 981(b) and criminal seizure warrants pursuant to Title 21 U.S.C. § 853(f) by Title 18 U.S.C. § 982(b)(1).

The application is based on these facts:
see Affidavit.

☒ Continued on the attached sheet.


Applicant's signature

Ricky Welton, Special Agent, U.S. Army CID
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/19/2020


Judge's signature

City and state: Waco, TX

Jeffrey C. Manske, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TEXAS
WACO DIVISION

IN THE MATTER OF THE SEARCH OF:
5007 Onion Road, Killeen, Texas

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, RICKY L. WELTON, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 5007 Onion Road, Killeen, Texas (**Texas Target Location #1**), further described in **Attachment A**, for the things described in **Attachment B**.
2. I have been a Special Agent with the Army Criminal Investigation Division (CID) Criminal Investigation Division in San Antonio, Texas since April of 2019. Prior to my employment with Army CID I was a Deputy U.S. Marshal from August 2006 through April 2019. During this time period, I have investigated violations of the federal laws and related offenses. As a Special Agent, I have investigated or been involved in investigations involving offenses under Titles 18, 21, and 42 of the United States Code.
3. I have provided investigative expertise and assistance to various agencies, including the Federal Bureau of Investigation (FBI); the United States Postal Service (USPS); Defense Criminal Investigative Service (DCIS); Texas Department of Public Safety (DPS); Drug Enforcement Agency (DEA) and various other law enforcement units of federal, state, county, and local governments, in their investigations of individuals who derive substantial income from the sale of stolen property, wagering, the sale/distribution of narcotics, the illegal export of property, structuring, and through the misappropriation of funds. My

assistance has included the documentation and tracing of illegal proceeds obtained in violation of various Federal and State statutes.

4. I have been the affiant in applications for numerous search/seizure warrants used to secure financial evidence and cellular phones involving narcotics, white collar fraud, money laundering, and other violations of federal law. I have also participated in debriefing/interviewing defendants, witnesses, informants, and other persons who have knowledge of the amassing, spending, converting, transporting, distributing, laundering and concealing the proceeds from the sale of stolen property, narcotics trafficking, and other illegal activities. I also have experience in investigating financial crimes committed by individuals who structure financial transactions, launder money through the use of nominees and shell corporations/businesses, and operate fraudulent schemes and structuring operations including violations of Titles 18, 21, and 42 of the United States Code. I have been previously assigned to a DEA Organized Crime Drug Enforcement Task Force in San Antonio, Texas as a Deputy U.S. Marshal investigating local and international drug organizations.

5. This affidavit conveys information provided by various federal and state law enforcement agencies, surveillance, and victim statements, and documents acquired during this investigation. Based upon the facts contained in this affidavit, I submit that there is probable cause to believe that located within the residences, vehicles and/or in the possession of persons described below and in attachments A (incorporated herein) there are currently evidence, fruits, and instrumentalities relating to a conspiracy to commit wire fraud, mail fraud, identity theft, theft of government funds, and money laundering by Kevin PELAYO (hereafter described as PELAYO), Cristine

FREDERICKS (hereafter described as FREDERICKS), and others known and unknown. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. Statements are related in sum and substance. Based on my experience and knowledge I know the following:

- a) That it is common for individuals engaged in mail and wire fraud, identity theft, and money laundering to maintain books, records, receipts, notes, ledgers, airline tickets, bus tickets, rental car receipts, receipts relating to the purchase of financial instruments, and or the transfer of funds, and other papers relating to the mailing of solicitations, purchasing, processing, and the collection of its proceeds. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the fraud and money laundering is facilitated so they have ready access to them and they are maintained for long periods of time;
- b) That it is common for individuals engaged in theft of government property, wire fraud, identity theft, and money laundering to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and or expenditure of illegal proceeds, such as: currency, financial instruments, precious metals and gem stones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, loan records, stored value cards, money orders, bank drafts, cashier checks, bank checks, wire transfers, safe deposit box keys, money wrappers, and records of their victims. These items are maintained by the persons perpetrating fraud within their residences, vehicles, and/or other locations which they maintain dominion and control over for long periods of time;

- c) That persons perpetrating theft of government funds, wire fraud, identity theft, and money laundering often utilize electronic equipment such as currency counting machines, telephone answering machines, telephone caller identification boxes, cellular telephones, smart phones, and pagers (digital display beepers) in their illegal activities;
- d) That persons perpetrating theft of government funds, wire fraud, identity theft, and money laundering often take or cause to be taken photographs/video of themselves, their associates, their property, and their products. These persons usually maintain these photographs, video tape, storage devices in their residences and/or other locations in which they maintain dominion or control;
- e) That persons perpetrating theft of government funds, wire fraud, identify theft, and money laundering commonly use portable electronic devices, such as cellular phones, smart phones, and tablet computers to carry-out, store and maintain records in regards to their business activities. Cell phones, smart phones, and tablet computers have evolved to the point that they are in essence miniaturized “computers” unto themselves; capable of performing many of the same functions – and in many cases altogether unique and different functions – as a traditional desktop or laptop computer. These devices allow users to conduct transactions and readily carry-out a variety of tasks from almost anywhere and at any time; and users often keep the devices on or near themselves at all times. These devices can store the same types of records that are stored on desktop and laptop computers, and they are often integrated with and capable of accessing the data and files contained on a user’s home and/or work computer systems. Updates that occur on one device can be accessible and available from any of the devices (computer, laptop, cell phone, and/or tablet device, etc.) connected to this network. Even the most basic cell

phones typically have the ability to make and receive text messages, take pictures, and/or access the internet even if only in a rudimentary manner. These individuals usually maintain these portable electronic devices in their possession, in their vehicles and/or at their residence, business, and/or organization.

OFFENSES ALLEGED IN THIS AFFIDAVIT

This affidavit provides probable cause to believe that KEVIN PELAYO and CRISTINE FREDERICKS, and others known and unknown to your affiant at this time, conspired to commit wire fraud, identity theft, theft of government funds, and to launder the illegal proceeds since at least on or before January 2014, continuing through the present.

There is probable cause to believe that evidence of wire fraud, theft of government funds, identity theft, and money laundering, as well as, attempts and/or conspiracies to commit these offences, in violation of Title 18, United States Code, Sections 641, 1343, 1028A, 1956h, and 371, respectively, will be found in the target locations.

ound in the target locations.

COMPUTER-RELATED ISSUES

Computers are Instrumentalities and Stored Evidence. I know based upon training and experience that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security

devices which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about crime.

Definitions

Definition of Computer

The term "computer," as used herein, is defined pursuant to Title 18, United States Code, § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

Computer hardware and computer software may be utilized to store records which include those related to business activities, criminal activities, associate names and addresses, and the identity and location of assets illegally gained through criminal activity. The terms records, documents, and materials include all information records in any form, visual or aural, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including the following:

- a. Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks statements, receipts, returns, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets; and,
- b. Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes, and aural records or representations, tapes, records, disks.

The term records, documents, and materials include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications that may have been created or stored, including: any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic forms (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, ZIP disks, CD-ROM disks, DVD disks, optical disks, printer buffers, smart cards, electronic dialers, or electronic notebooks, tapes, flash or thumb drives, personal digital assistants, digital video recorders, memory sticks, as well as printouts or readouts from any magnetic storage device).

Definition of Computer Hardware.

Computer hardware which consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes any data-processing devices (such as central processing units, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, network routers or hubs, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices,

and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Definition of Computer Software.

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

Internet.

The Internet is a global computer network which electronically connects computers and allows communications and transfers of data and information across state and national boundaries. To gain access to the Internet, an individual utilizes an Internet service provider (ISP). These ISP's are available worldwide. When an individual communicates through the Internet, the individual leaves an Internet Protocol (IP) address which identifies the individual user by account and ISP.

Computer Documents.

Computer-related documentation which consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

Computer Security.

Computer passwords and other data security devices which are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric

characters usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

Seizure of Electronic Storage Devices.

Based upon your affiants knowledge, training and experience, and consultations with Brian Janco Digital Forensic Examiner with the U.S. Army Criminal Investigation Division, your affiant knows that the search and seizure of information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following.

The volume of evidence.

Computer storage devices (like hard disks, diskettes, tapes, laser disks, RAID arrays) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

Technical requirements.

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even “hidden”, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

Procedures for Seizing Electronic Data.

Based upon your affiants knowledge, training and experience, and consultation with Brian Janco, Digital Forensic Examiner with the U.S. Army Criminal Investigation Division, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system’s input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. This is true because of the following:

The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or “I/O”) devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs

the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as, all related instruction manuals or other documentation and data security devices.

Request to Move Computers Off-Site To Search Before Return.

Therefore, your affiant requests that your affiant be permitted to remove the computer hardware, computer software, disks, instruction/operating manuals, peripherals, and interconnecting cable/wire to an off site location where the computers can be searched, and the information authorized to be seized by this warrant downloaded and copied.

PROBABLE CAUSE

The purpose of the Department of the Army's Mass Transportation Benefit Program (MTBP) is to reduce Federal employees' contribution to traffic congestion and air pollution and to expand their commuting alternatives by using mass transportation. Presidential Executive Order 13150, subject Federal Workforce Transportation, dated 21 April 2000, directs all Federal agencies to implement a Mass Transportation Benefit Program to qualified Federal employees for individual employee commuting costs incurred through the use of mass transportation and van pools. The Department of the Army (DA) implemented its Mass Transportation Benefit Program effective 1 January 2001, for Army soldiers and civilian employees.

The U.S. Department of Transportation (DOT) serves as the Executive Agent for all Federal agencies, including Army. DOT handles all administrative aspects involved with the purchase and distribution of fare media. Under the MTBP, the Army provides transportation subsidies to soldiers and civilian employees, using direct deposit for distributing fare media.

Fare media varies based on the location and type of mass transportation used. Fare media is distributed every month basis. An allotment of fare media is provided to program participants at the beginning of each time period for that time period. Electronic fare media, allotment is made via the applicable automated system each month. Chase Paymentech is the processing and merchant acquiring business of JPMorgan Chase.

JPMorgan Chase Paymentech provides electronic payment products for businesses that accept credit, debit or gift cards from their customers. Soldiers Van Pools, LLC uses JPMorgan Chase Paymentech for their business as indicated on their Merchant Business application that was submitted on December 02, 2013 by Kevin PELAYO.

Point of contacts (POC) will complete the point of contact registration form and send it to the Department of Transportation Army Account Manager to represent the local installation as the MTBP point of contact.

POCs accept applications for enrollment in the MTBP, review the applications for accuracy, verify and approve applicants' eligibility to participate in the program, review applicants' calculation of commuter expenses, and submit the applications using the MTPB Application Submission Form (Excel spreadsheet). Outgoing POCs are responsible for the effective turnover of the program to the incoming POC.

Additionally, the POC has to maintain up-to-date, concise records which provide a historical perspective of all participants' pick-up records along with the amount of fare media received. The tracking system should also document participants' failure to adhere to the distribution policy. The POC should retain these records on file for at least one year from the distribution dates.

POCs have to maintain an internal tracking system of participants and keep participants' original and updated application forms on file at the installation for as long as the individual remains enrolled in the program. When an individual withdraws from the program, the application files should be kept on file for one year after the date of withdrawal. These files must be properly secured, as they contain personal information.

Section II of the application form requires the applicant's signature/initials for each item. Section V also requires the applicant's signature, as well as the signature of his/her supervisor. These items may either be signed digitally or manually. Participants must submit a withdrawal application if they choose to withdraw from the program, or when they depart from their installation. Departure includes retirement, separation, dismissal and transfer. If a participant is changing locations, the participant must withdraw from the location and re-enroll with the POC at their new location. The applicant's signature in Section V of the application form certifies that the information provided on the form is true and correct.

Van pool pricing models vary between providers, but in most cases, van pools charge a monthly fee for the vehicle, consisting of the fixed and variable costs for that month. Participants calculate their claimed benefit amount based on the total number of seats in the van pool, not the number of riders. The mass transportation benefit is not to be used to offset the cost of empty seats in the van.

Summary of Scheme

On, before, or about January 2014, and continuing through the present, PELAYO & FREDERICKS have been operating an illegal scheme(s) within the Western District of Texas

and elsewhere. One of the illegal scheme(s) involves obtaining soldiers names and personal identifiable information to send to the Department of Transportation to claim a payment upon their behalf to be sent directly to PELAYO & FREDERICKS JP Morgan Chase Business account under the name Soldiers Vanpools, LLC. The payments were received by PELAYO's merchant business account.

On or about December 2013 Kevin PELAYO submitted a merchant application and agreement through CHASE Paymentech. This application is for a merchant Business and federal regulations require banks to collect and retain information verifying merchant's identity. Kevin PELAYO stated Soldiers Vanpools, LLC is a Merchant business with a prior residential address of 4501 Lonesome Dove Drive, Killeen, Texas 76549. Telephone number 253-232-5392, merchant business email address as kevinpelayo@hotmail.com. Kevin PELAYO stated that his business Soldiers Vanpools, LLC was not home-based and stated that Soldiers Vanpools, LLC was a retail business and provided transportation/vanpool services and was not a seasonal business. Additionally, Kevin PELAYO stated on the sales information that his business does not ever charge a customer on a recurring basis and that the Soldier Vanpools, LLC estimated annual breakdown in % of annual payment card transactions was 100%.

The transactions going into his bank accounts were in multiple sums and on a monthly basis of up to \$25,000 at a time which are represented in PELAYO and FREDERICKS's JP Morgan Chase Bank account XXXX2010 and at times exceeded \$200,000 a month in deposits.

SA Welton along with SA Benefield was able to interview numerous soldiers, who will hereafter be described as (victim 1, etc) on the lists of participants that were provided by Army Finance Command. Additionally, SA Welton has interviewed several individuals who will hereafter be described as cooperating witnesses (cw 1, etc) who have provided information.

Several victims interviewed stated that they were not aware of being a participant in the program and stated that they did not authorize PELAYO to use their names or PII to claim a benefit to go to Soldiers Van Pools, LLC from September 2018 through September 2019. SA Welton believes that PELAYO was able to gather and obtain the names and PII of numerous soldiers due to his position as a platoon sergeant. As a platoon sergeant, PELAYO had access to personnel files that contained their military records to include PII. A number of soldiers interviewed were unaware of being a MTBP participant on Ft. Hood, Texas from September 2018 through September 2019 based on the records received from Army Finance Command and JPMorgan Chase.

SA Welton believes that PELAYO then used the names of soldiers and their PII by obtaining the information from their personnel record, utilizing his company Soldiers Van Pools, LLC as their transportation provider. PELAYO then emailed an excel spreadsheet to the Department of Transportation every month from September 2018 through July 2019 with the names of U.S. Army Soldiers as alleged participants for the Ft. Hood, Texas Mass Transportation Benefit Program (MTBP). Once the Department of Transportation received the excel spreadsheet from PELAYO with the names of the alleged participants, the Department of Transportation would input their names and information into a database as a participant for the program utilizing Soldier Van Pools, LLC as their van pool service provider.

In order for PELAYO to do this, PELAYO had to obtain the names and personal information from each soldier and personally fill out a standard application form which included their full name, last four of SSN, residence city, state, duty location, office telephone number, work email address, supervisor name, van pool coordinator, van pool id, vanpool vehicle license plate, name of mass transit system or company participant intends to use, specific fare media type (debit card, voucher, etc).

PELAYO bypassed the proper steps for the application procedures and just sent the Excel spreadsheet directly to the Department of Transportation for processing.

Additionally, it was the responsibility of the soldier to fill out the transportation benefit calculation as indicated on the application form to determine the amount per month the applicant is authorized to receive. PELAYO set every participant up to receive the maximum amount authorized which was either \$255 or \$265 depending on the time they were processed.

Each card was set up to the vanpool provider so that every month the determined amount on the application was debited directly to the vanpool provider. PELAYO set up each applicants Trans-Serve card to go directly to his bank account every month in the amount of either \$255 or \$265 per participant as reflected in his business account and records received by JPMorgan Chase.

This created substantial income for PELAYO and FREDERICKS outside of their normal military pay, retirement and disability checks from January 2014 through December 2019, which sometimes exceeded \$200,000 a month going directly into their JP Morgan Chase business account. Once the payments were deposited, the funds were transferred to various bank accounts by PELAYO and FREDERICKS. The funds were traced under the Financial Analysis of Bank Accounts section of this affidavit. The soldiers that were submitted by Kevin PELAYO had their identities stolen. Additionally, their stolen identities were then used to file fraudulent participant application forms for the benefit of PELAYO and FREDERICKS. Moreover, PELAYO and FREDERICKS had bank accounts into which fraudulent payments were deposited. PELAYO, and FREDERICKS then withdrew the illegal proceeds. Additionally, FREDERICKS became the Owner of Soldier Van Pools, LLC on or around June 2018 based on records obtained from the Texas Comptroller's Office and should have kept a record of all participants that were signed up

utilizing Soldier Van Pools, LLC. It was also known that PELAYO would send some of the proceeds via Western Union to the Philippians, to an unknown person, all in violation of Title 18, United States Code, Sections 641, 371, 1343, 1956(h), and 1028A.

Your affiant states that the facts which establish probable cause necessary for the issuance of search warrants for 5007 Onion Road, Killeen, Texas (**Texas Target Location #1**).

The Investigation

A. Special Agent Ricky Welton has been a Special Agent with the United States Army Criminal Investigation Division (CID) since April 2019. Prior to my employment with CID I was a Deputy U.S. Marshal for over (13) years. Special Agent Welton has participated in investigations involving offenses related to United States Code 18, 21, and 42, to include: wire fraud, identity theft, narcotics trafficking, and money laundering.

1. CW-1, Army Finance Command, provided information to CID Special Agent Perkins assigned to the Ft. Hood, Texas CID Office on or about October 1, 2019. SA Welton has also interviewed CW-1 on December 10, 2019. CW-1's information is considered to be credible and reliable and has been corroborated by Special Agents, soldier statements, surveillance, and documents inspected during this investigation. The information from CW-1 is in sum and substance as follows:
2. Special Agent Abraham Perkins, Ft. Hood, Texas CID Office, was notified by CW-1, Financial Management Systems Analyst, Army Financial Services, USAFMCOM, Indianapolis, IN that SFC (now SFC (Ret)) Kevin PELAYO may have committed fraud and stolen funds from the government while serving as the Local Program Manager/Point of Contact for the Mass Transportation Benefit Program (MTBP). CW-1 stated his office attempted to coordinate with the Local Program Manager (LPM) at Fort Hood, TX.

However, attempts to contact the LPM via email were unsuccessful. CW-1 stated his office then contacted the owner of the local van pool, at which point they realized SFC Kevin PELAYO was both the LPM and the owner of the local van pool company, Soldiers Vanpools LLC. CW-1 stated SFC Kevin PELAYO retired on 1 Aug 19. SA Welton was able to verify this information through U.S. Army Personnel Records. CW-1 stated that SFC PELAYO shredded the attendance schedules and all associated documents for the local MTBP participants that PELAYO was overseeing. CW-1 stated his office spoke with a CW-2, who related he was previously a participant in the MTBP but was not physically present at Ft. Hood, Texas during a period SFC PELAYO may have reported CW-2 was utilizing the van pool services. CW-1 stated he did not have an estimate regarding total potential loss to the government at the time.

3. On or about Oct 2, 2019, Special Agent Perkins coordinated with CW-1 who confirmed the funding for the MTBP comes from the Department of Defense (DOD). CW-1 stated he does not know how SFC PELAYO could have been serving as the Local Program Manager for Ft. Hood, Texas while stationed in South Korea. Kevin PELAYO last duty station was South Korea. Kevin PELAYO was stationed in South Korea in 2018 until he retired on or around August 1, 2019.
4. On or about October 16, 2019, Special Agent Perkins received an email from CW-1 which contained an attached Excel spreadsheet. The spreadsheet shows the FY19 billing totals for the Ft. Hood, Texas MTBP. A review of the spreadsheet indicated the total amount processed through the Ft. Hood, Texas MTBP for FY19 was approximately \$2.3 million dollars. Special Agent Perkins coordinated with Special Agent Ricky Welton, Major Procurement Fraud Unit, San Antonio, Texas to work on case transfer from the Ft.

Hood, Texas CID Office to the Major Procurement Fraud Unit due to amount of money involved, resources, and possible loss to the Army.

5. Special Agent Perkins coordinated with CW-2 on December 3, 2019 who stated that he was unaware of a physical office location for the Ft. Hood, Texas MTBP. CW-2 stated SFC (Ret) PELAYO kept all the vehicles at the driveway of his residence.
6. Special Agent Welton spoke to CW-1 on December 10, 2019 in reference to the excel spreadsheets that was originally sent to Special Agent Perkins. CW-1 explained that the spreadsheets were generated based off of the participants associated with Kevin PELAYO and the monthly transactions that were being charged per participant during the time that the participant was enrolled in the program. Special Agent Welton was able to determine based off of the charts that majority of the participants received on average \$255 a month that went directly to Soldiers VanPools, LLC, a company owned and operated by PELAYO and FREDERICKS.
7. On February 6, 2020, Victim 1, an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$3,000 in payments to Soldiers Van Pools LLC were associated with victim 1's PII. Victim 1 currently serves on active duty at Ft. Gillem, GA. Victim 1 denied he ever participated in the MTBP and denied that he ever authorized anyone to use his PII for payments to Soldiers Van Pools LLC during this time. Victim 1 stated has never been stationed on Ft. Hood, Texas.
8. On February 10, 2020, victim 2 was interviewed as an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$3,300 in payments to Soldiers Van Pools LLC were associated

with victim 2's PII. Victim 2 currently serves on active duty at Joint Base Elmendorf, Alaska. Victim 2 denied he was a participant in the MTBP during this time and denied he authorized anyone to use his PII for payments to Soldiers Van Pools LLC during the time he was stationed at Ft. Hood, Texas or any other time.

9. On February 20, 2020, victim 3 was interviewed as an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$2,800 in payments to Soldiers Van Pools LLC were associated with victim 3's PII. Victim 3 currently serves on active duty at Ft. Bliss, Texas. Victim 3 denied he ever participated in the MTBP or that he authorized anyone to use his PII for payments to Soldiers Van Pools LLC during the time he was stationed at Ft. Hood, Texas or any other time.
10. On March 19, 2020, victim 4 was interviewed as an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$3,000 in payments to Soldiers Van Pools LLC were associated with victim 4's PII. Victim 4 currently serves on active duty at Ft Sam Houston, Texas. Victim 4 denied he ever participated in the MTBP or that he authorized anyone to use his PII for payments to Soldiers Van Pools LLC during the time he was stationed at Ft. Hood, Texas or any other time.
11. On March 19, 2020, victim 5 was interviewed as an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$3,000 in payments to Soldiers Van Pools LLC were associated with victim 5. Victim 5 currently serves as a Reservist in the U.S. Army. Victim 5 denied he ever participated in the MTBP or that he ever authorized anyone to use his PII for

payments to Soldiers Van Pools LLC during the time he was stationed at Ft. Hood, Texas or any other time.

12. On March 20, 2020, victim 6 was interviewed as an alleged participant in the MTBP on Ft. Hood, Texas from approximately September 2018 through September 2019 for which approximately \$3,000 in payments to Soldiers Van Pools LLC were associated with victim 6. Victim 6 currently serves on active duty at Ft. Irwin, CA. Victim 6 denied he ever participated in the MTBP or that he ever authorized anyone to use his PII for any payments to Soldiers Van Pools LLC during the time he was stationed at Ft. Hood, Texas or any other time.
13. Special Agent Welton reviewed the names and records of numerous soldiers that were on the Ft. Hood, Texas Mass Transit Benefit Program that were associated with Kevin PELAYO and his business Soldiers Vanpools, LLC. It was determined by the interviews conducted that majority of the soldiers were not on Ft. Hood, Texas at the time these transactions were going into PELAYO's business account. Many soldiers were stationed at other U.S. Army Bases throughout the United States.
14. On or around June 2018, FREDERICKS became the owner of Soldier Van Pools, LLC and PELAYO was named the Director. This is based off of records obtained from the Texas Comptroller's Office.
15. Military records obtained by SA Welton indicate that while FREDERICKS was in the Army she worked in Human Resources and received training on how to maintain military records. Additionally, PELAYO was a platoon sergeant during the time the submissions to DOT were sent. As a platoon sergeant, PELAYO would have to update and document forms in the military records of the soldiers that he was in charge of. Having access to

soldiers military records provided PELAYO with the names and PII of soldiers under his command.

- B. Your affiant based on my training and experience in similar investigations, believes PELAYO and FREDERICKS, and unknown coconspirators were likely utilizing internet based systems to send and correspond with each other.
- C. Special Agent Welton along with Agents of the Texas Department of Public Safety were able to monitor the residence of Kevin PELAYO and Cristine FREDERICKS.
- D. The witness statements, set out below, suggest that the suspects knew the vehicles owned, operated and in their possession are vehicles I have not seen in person but through investigation of different sources believe them to be sold from the targets stock. Through surveillance and investigation, I do believe the targets are liquidating the vehicles they own through a variety of car companies in order to stay under the radar. They are prepping the vehicles thoroughly and removing license plates before the sale. Special Agent Welton believes at the residence Agents will find a number of License Plates at the residence to include service records from outside Texas near other military installations and identify possible co-conspirators.
 - 1. On March 24, 2020, Special Agent Welton along with the Texas Department of Public Safety agents observed PELAYO and FREDERICKS prepare several vehicles located at their residence to be transported. Carvana, a business that buys vehicles was seen loading up a Ford SUV on the bed of a Carvana flatbed truck to haul away. Additionally, PELAYO was seen loading up a White Dodge Durango onto a flatbed trailer to be hauled away. The trailer was hooked up to a White 4 door Ford pick-up truck that was driven by PELAYO. FREDERICKS was seen driving a Black Ford Explorer. All vehicles were driven to a parking lot operated by Carvana in Austin, Texas.

2. Additionally, agents were able to discover that three known Ford Explorers were sold to Hertz in Killeen, Texas. These vehicles were known vehicles of PELAYO and FREDERICKS because the vehicles were registered to either PELAYO or FREDERICK's right before the sale of the vehicles. Each vehicle was identified by their VIN number that was registered by them at their residence which is also their business address.

Department of Defense
United States Army

3. Your affiant reviewed Agent reports, to include, numerous interviews which, in sum and substance, reveal the following:
 - a. On or around December 10, 2019, Army Finance Command advised Army CID Special Agent Welton that PELAYO was contacted by the U.S. Army Finance Command due to irregularities with the Ft. Hood, Texas Army Mass Transit Benefit program. Agents knew that Kevin PELAYO was stationed at Camp Humphreys, South Korea in 2018 until his retirement in 2019. It is alleged that PELAYO and FREDERICKS knew that the information that was sent to the Department of Transportation was fraudulent but decided to keep their business going with illicit funds received by the U.S. Army. It is alleged that PELAYO knew the program very well due to his extensive involvement going back to 2014 when PELAYO was the MTBP POC stationed in Hawaii. Agents with Army CID know that an active duty soldier cannot afford the number of vehicles and properties on an E-7 pay. Records indicate that in July 2019, PELAYO made approximately \$3,450 in pay and that FREDERICKS receives a disability check for approximately \$800.
 - b. For FY 19, Special Agent Welton determined that PELAYO and FREDERICKS had approximately 84 vehicles registered to their name. Majority of the vehicles were not

seen at the residence at 5007 Onion Road, Killeen, TX (**Target Address #1**), even though they showed to be registered to either PELAYO or FREDERICKS. Additionally, Special Agent Welton was able to determine that PELAYO and FREDERICKS may have up to 22 properties in their name throughout Central Texas, Hawaii, New York, and Washington State as of June 1, 2020 based on certified title checks by IRS-CID.

c. Agent Welton along with the Texas Department of Public Safety and IRS believe that PELAYO and FREDERICKS bought and sold dozens of vehicles and purchased properties with the money received from the U.S. Army.

d. According to financial records, it is determined that the U.S. Army may be at a loss of approximately \$2.3 million and up to \$11.3 million or more.

4. Your affiant reviewed a report by Special Agent Neff detailing the bank accounts associated with PELAYO and FREDERICKS which is summarized in sum and substance as follows:

Financial Analysis of Bank Accounts

- A. Special Agent James Neff has been a special agent with IRS Criminal Investigations for approximately thirty-three (33) years. As an IRS Special Agent, he has investigated or been involved in investigations involving offenses under Titles 18, 21, 22, 26, 31, and 50 of the United States Code. Special Agent Neff has investigated financial crimes committed by individuals who structure financial transactions, launder money through the use of nominees and shell corporations/businesses, and operate fraudulent schemes. Several seizures of assets such as real estate, automobiles, bank accounts, currency, aircraft, oil wells, jewelry, computers, and other business equipment have resulted from these investigations. Special Agent Neff reviewed information from PELAYO's bank accounts at JP Morgan Chase Bank (Chase Bank), USAA Federal Savings Bank (USAA), Navy Federal Credit Union Navy FCU), Wells Fargo Bank and

Hickam Federal Credit Union (Hickam FCU) which he summarized in sum and substance as follows:

JP Morgan Chase Bank

1. Chase Bank checking account 551932010 under the name of Soldiers Vanpools LLC., was opened on or about January 13, 2014. The signatory on the account is shown as being Kevin PELAYO. On or about August 8, 2014, Cristine FREDERICKS was added to the account as a signatory according to the signature card.

- a. An analysis of Chase Bank account ending in 2010 revealed that the majority of the deposits into the account were from Paymentech. From 2014 through 2019, in excess of \$11.3 million was deposited into the account from Paymentech.
- b. The funds deposited into checking account ending in 2010 were used to make the payments on numerous mortgages and/or other loans through Wells Fargo Bank, Ally, Pentagon Federal, and Vistana as well as payments to credit card accounts, automobile finance companies, ATM withdrawals, and personal living expenses during 2014 through 2019. The funds were also used to purchase vehicles and other assets as follows:

Year	Company Name	Amount
2017	Monteith Abstract & Title	\$ 351,428.00
2017	Texas Sunrise Solars	\$ 17,000.00
2017	Ronald Esposito*	\$ 225,000.00
2019	Martinka Construction	\$ 184,000.00
2019	Avis Car Sales	\$ 94,000.00
2019	Hertz Car Exchange	\$ 196,000.00
2019	Johnson Ford	\$ 76,000.00

* PELAYO sent five (5) wire transfers totaling \$225,000 to Ronald Esposito as part of the purchase of his residence at 5007 Onion Road, Killeen, Texas in 2017.

c. The deposited funds were also transferred electronically and/or with cashier's checks purchased from Chase Bank account ending in 2010 to various bank accounts controlled by PELAYO and/or FREDERICKS at Chase Bank and USAA as follows:

1. Funds were transferred electronically to Chase Bank checking account ending in 0670 in excess of \$3.5 million from January 2017 through December 2019.
 2. Funds were transferred electronically to Chase Bank account ending in 9757 for approximately \$18,000 in 2018 and 2019.
 3. Funds were transferred electronically to USAA saving account ending in 4387 in excess of \$620,000 from January 2016 through August 2018.
 4. Funds were transferred electronically to USAA checking account ending in 4395 in excess of \$100,000 from January 2016 through August 2018.
 5. Cashier's checks were purchased using funds from account ending in 2010 which were deposited into USAA accounts ending in 9945 and 9937 for a total of \$26,000 in 2017 and 2019.
2. Chase Bank checking account ending in 6801310670 is under the signatory names of Kevin PELAYO, Cristine FREDERICKS, and Edna Pelayo. The signatory card was dated on or about December 16, 2015.
- a. An analysis of Chase Bank checking account ending in 0670 revealed that besides the \$3.5 million in funds deposited into the account from Chase Bank account ending in 2010 (Soldiers Vanpools LLC), in excess of \$640,000 in cash was also deposited into

the account from January 2017 through December 2019. The funds deposited into the account were used to purchase numerous assets expended or transferred as follows:

- b. Funds transferred from Chase Bank checking account ending in 2010 were used for personal and business expenditures. A summary of the assets and large expenditures from account ending in 0670 for the years 2017, 2018, and 2019 is shown as follows:

Company	Total Amount	
Johnson Brother's Ford	\$ 702,000.00	
A-1 Fence	\$ 22,000.00	
Martinka Construction	\$ 492,000.00	
Sunrise Solar	\$ 65,000.00	
American Abstract	\$ 149,000.00	
Monteith Abstract & Title **	\$ 780,000.00	
Dreyfus Family of Funds *	\$ 68,000.00	
Hertz Car Exchange	\$ 189,000.00	
Ford Credit	\$ 100,000.00	

* The checks written to Dreyfus Family of Funds had the account number 0255-3360205490 written in the memo section of each personal check. Internet research revealed that the Dreyfus Family of Funds is operated by the Bank of New York.

** Deed records revealed that PELAYO and FREDERICKS purchased their residence at 5007 Onion Road, Killeen, Texas from Ronald Esposito on or about June 9, 2017. On June 8, 2017, a cashier's check made payable to Monteith Abstract & Title was purchased for \$296,694.

- c. The deposited funds were also transferred via cashier's checks and/or personal checks, made payable to PELAYO, drawn on Chase Bank account ending in 0670 to various bank accounts controlled by PELAYO at USAA and Navy FCU as follows:
1. In 2018, two (2) personal checks were made payable to PELAYO for \$100,000 each. Both checks were deposited into PELAYO's Navy FCU account ending in 5291.

2. At least twenty-six (26) cashier's checks totaling in excess of \$160,000 were purchased with funds from account ending in 0670. These checks were traced being deposited into USAA accounts ending in 9945 and 9937 during 2018 and 2019.
3. In 2018, seven (7) personal checks were made payable to PELAYO for \$100,000 each totaling \$700,000. Six (6) of the checks were deposited into USAA checking account ending in 4395 and one (1) check was deposited into USAA savings account ending in 4387.

USAA Bank

3. Kevin PELAYO is the signatory on USAA checking account 0041534395. The signatory card was dated on or about April 19, 2007. The account is summarized as follows:
 - a. Funds in excess of \$680,000 were received into this account via electronic transfer and personal checks, made payable to PELAYO, from Chase Bank accounts 2010 and/or 0670. Additionally, personal checks in the name of Kevin PELAYO and made payable to PELAYO were deposited into this account totaling \$350,000 drawn on bank accounts at Navy FCU, Hickam FCU, and Wells Fargo Bank. Funds in excess of \$370,000 were also transferred into this account from USAA savings account ending in 4387.
 - b. From July 2018 through December 2019, in excess of \$850,000 was also electronically transferred to two (2) USAA Investment Management Company (IMCO) accounts, RNQ588252 and MNQ077300. These accounts are now managed by Victory Capital Management, Inc. The transfer records show that the transfers were credited to PELAYO. During the same timeframe, approximately \$616,000 was transferred back into account ending in 4395.

c. The funds deposited into this account were used for personal living expenses, to purchase large assets, and transferred to other bank accounts believed to be controlled by PELAYO and/or FREDERICKS from January 2017 through February 2020, as follows:

1. The funds were traced as follows:

Company	Amount
Hertz Car Exchange	\$ 120,000.00
Johnson Brothers Ford	\$ 24,000.00
Martinka Construction	\$ 32,000.00
Bank of New York - Mutual Funds	\$ 48,000.00
Crestview RV	\$ 14,487.00
Ford Motor Credit	\$ 154,000.00

2. Personal checks made payable to Kevin PELAYO totaling in excess of \$250,000 were deposited into PELAYO's account at the Navy FCU.

4. Kevin PELAYO is the signatory on USAA savings account 0041534387. The signatory card was dated on or about April 19, 2007. The account is summarized as follows:

- a. Funds in excess of \$720,000 were received into this account via electronic transfer and personal checks, made payable to PELAYO, from Chase Bank checking accounts 2010 and/or 0670 from January 2016 through August 2019.
- b. In excess of \$370,000 was electronically transferred to USAA checking account ending in 4395.
- c. Additionally, approximately \$269,000 was also electronically transferred to IMCO account RNQ588252. The transfer records show that the transfers were credited to PELAYO. During the same timeframe, approximately \$5,000 was transferred back into account ending in 4387.

5. Cristine FREDERICKS is the signatory on USAA checking account 01552-3994-5. The signatory card was dated on or about March 21, 2013. The account is summarized as follows:
 - a. Funds in excess of \$174,000 were received into this account via cashier's checks, made payable to FREDERICKS, purchased from Chase Bank accounts 2010 and/or 0670 from January 2017 through August 2019. In excess of \$20,000 cash was deposited and in excess of \$19,000 was electronically transferred into the account from USAA savings account ending in 9937.
 - b. The majority of these funds appear to have been used for personal living expenses including in excess of \$180,000 expended at Neiman Marcus clothing store.
6. Cristine FREDERICKS is the signatory on USAA savings account 01552-3993-7. The signatory card was dated on or about March 21, 2013. Cashier's checks, made payable to FREDERICKS, purchased from Chase Bank accounts 2010 and/or 0670 totaling \$20,000 were deposited into this account from January 2017 through August 2019. The majority of these funds were transferred into USAA account ending in 9945.

Navy FCU

7. Kevin PELAYO is the signatory on Navy FCU savings account 3077585291 and checking account 7059884721. The signatory card was dated on or about November 23, 2016. The accounts are summarized as follows:
 - a. Funds in excess of \$210,000 were deposited into the Navy FCU savings account from Chase Bank account ending in 0670 in 2017 and 2018. Funds in excess of \$250,000 were deposited into the Navy FCU savings account from USAA account ending in 4395

in 2017 and 2018. Additionally, approximately \$34,000 cash was deposited into the account from 2017 through 2019.

b. The majority of the funds deposited into the Navy FCU savings account was transferred to the Navy FCU checking account ending in 4721. In excess of \$135,000 cash was withdrawn from the account. Additionally, \$250,000 in checks made payable to PELAYO was deposited into the USAA account ending in 4395 in 2019.

ASSETS TO BE SEIZED

The following financial accounts were discussed above and proceeds from the fraudulent scheme were traced into each of the accounts.

JP Morgan Chase Bank, checking account number 551932010

JP Morgan Chase Bank, checking account number 6801310670

USAA Federal Savings Bank, checking account number 004153439-5

USAA Federal Savings Bank, savings account number 004153438-7

USAA Federal Savings Bank, checking account number 01552-3994-5

USAA Federal Savings Bank, savings account number 01552-3993-7

Victory Capital Management, Inc. account RNQ588252

Victory Capital Management Inc. account MNQ077300

Navy Federal Credit Union, checking account number 7059884721

Bank of NY Mellon (Dreyfus Funds), mutual funds 0255-3360205490

**White 2018 Ford F250 Pickup, Texas License 4DV1869,
VIN: 1FT7W2BT9JEC18474, Registered to Kevin PELAYO**

**2019 Cougar 32B Travel Trailer, Texas License B408801, VIN: 4YDF32B23K2511637,
Registered to Kevin PELAYO**

**Gray 2020 Ford Explorer SUV, Texas License 3DV3514, VIN: 1FMSK8DH0LGA91649,
Registered to Kevin PELAYO**

Silver 2018 Chevy Silverado Pickup, Texas License MHX3978,
VIN: 3GCUKRECXJG448780, Registered to Kevin PELAYO

Red 2018 Chevy Pickup, Texas License MHX4700, VIN: 1GCUKREC4JF172579,
Registered to Kevin PELAYO

Black 2018 Big Tex Flatbed Trailer, Texas License 104025K, VIN: 16VCX1825J3009351,
Registered to Kevin PELAYO

Black 2019 Chrystler Minivan, Texas License 3DV2045, VIN: 2C4RC1N79KR590380,
Registered to Kevin PELAYO

White Ford Transit Bus, Texas License 4DV1709, VIN: 1FBAX2CGXKKA94212,
Registered to Kevin PELAYO

White Chrysler Minivan, Texas License FYL7783, VIN: 2C4RC1BG9FR545224,
Registered to Kevin PELAYO

Black Chevy Tahoe, Texas License MHX3766, VIN: 1GNSKBKC1KR160917,
Registered to Cristine Fredericks

Black Tesla, Texas License NHY5174, VIN: 5YJSA1E23JF281638,
Registered to Cristine Fredericks

Polaris ATV, VIN: 4XAT6E997L8875115, Registered to Cristine Fredericks

Polaris ATV, VIN: 4XAT6E994L8879865, Registered to Cristine Fredericks

SURVEILLANCE

8. Your affiant and agents with the Texas Department of Public Safety have conducted surveillance on numerous occasions at 5007 Onion Road, Killeen, Texas (**Texas Target Location #1**) from January 2020 through June 2020. The surveillance observations are summarized in sum and substance as follows:

1. A 2019 black Chevy Tahoe bearing Texas License MHX3766, a 2018 white Ford F-250 bearing Texas license 4DV1869, a 2019 beige multi-color Cougar Travel Trailer bearing Texas license B408801, a gray 2020 Ford Explorer bearing Texas license 3DV3514, a 2018 silver Chevy Silverado bearing Texas license MHX3978, a red 2018 Chevy

Silverado bearing Texas license MHX4700, a 2018 black Big Tex flatbed trailer bearing Texas license 104025K, a 2019 black Chrysler minivan bearing Texas license 3DV2045, a 2019 white Ford Transit bus bearing Texas license 4DV1709, and a white Chrysler minivan bearing Texas license FYL7783 along with a maroon color Chevy four door pickup, a Tesla Model S with paper license plates, and other vehicles registered to PELAYO and FREDERICKS have been observed at 5007 Onion Road, Killeen, Texas (**Texas Target Location #1**) on numerous occasions throughout the investigation but most recently on June 3, 2020.

9. Your affiant reviewed internet databases which revealed that 5007 Onion Road, Killeen, Texas (**Texas Target Location #1**) was purchased by Kevin PELAYO and Cristine FREDERICKS for \$343,750 on June 9, 2017.
10. Your affiant reviewed the Texas Comptroller's Office records in order to verify the business address for Soldiers Vanpools, LLC. SA Welton was able to determine based off of the Texas Franchise Tax Public Information Report that on May 11, 2018 PELAYO submitted that FREDERICKS is the owner of Soldiers Vanpools, LLC at 5007 Onion Road, Killeen, Texas 76542 (**Texas Target Location # 1**). Records also show as of November 12, 2018 that FREDERICKS is the owner of Soldiers Vanpools, LLC and PELAYO is the Director of Soldiers Vanpools, LLC at 5007 Onion Road, Killeen, Texas 76542 (**Texas Target Location # 1**).
11. Your affiant reviewed the Texas Workforce Commission (TWC) records in order to verify employment history for PELAYO and FREDERICKS. The documents revealed the following in sum and substance:
 1. PELAYO showed no TWC wages earned. There are no reported wages for PELAYO in 2018-2019.

2. FREDERICKS (PELAYO's wife) shows no TWC wages earned. There are no reported wages for FREDERICKS in 2018-2019.

Criminal Histories

12. Your affiant reviewed law enforcement databases which reveals the following criminal history for PELAYO and FREDERICKS in sum and substance:

- A. No criminal history has been found for PELAYO or FREDERICKS

SUMMARY

Your affiant believes that PELAYO and FREDERICKS, and others known and unknown are and have been orchestrating a scheme to defraud the U.S. Army throughout the Western District of Texas and beyond by obtaining the names of soldiers and then submitting the names of the soldiers to the Department of Transportation for the Ft. Hood, Texas Mass Transit Benefit Program to have a monthly payment direct deposited into their bank account with the soldiers having no knowledge of their participation in the program. SA Welton believes that numerous U.S. Army Soldiers had their names and personal identification information used by PELAYO to claim a monthly payment without their knowledge, consent, or authorization. SA Welton believes that through bank records, interviews, and documents that PELAYO and FREDERICKS fraudulently obtained up to \$11.3 million dollars or more from this program. SA Welton has also shown that millions of dollars were being transferred between bank accounts and to individuals known and unknown and that hundreds of thousands of dollars have been transferred into retirement accounts. Your affiant has shown that majority of the proceeds was used to buy vehicles and properties throughout the United States, specifically 5007 Onion Road, Killeen, Texas (**Texas Target Location # 1**) and other properties in Texas, Hawaii, New York, and Washington State. SA Welton believes he has shown PELAYO conspiring with other people

known and unknown to defraud the U.S. Army out of millions of dollars. SA Welton was able to show this based off of bank record analysis conducted by the Internal Revenue Service (IRS). SA Welton has also shown through documents provided by the Texas Comptroller's Office and Department of Defense records that PELAYO and FREDERICKS have used 5007 Onion Road, Killeen, Texas (**Texas Target Location # 1**) as their home and Business since June 2017. SA Welton and the Texas Department of Public Safety agents have also seen PELAYO move several vehicles at 5007 Onion Rd, Killeen, Texas (**Texas Target Location # 1**). Your affiant believes that PELAYO and FREDERICKS are utilizing their persons, vehicles, and residence (**Texas Target Location # 1**) to maintain, facilitate, and orchestrate the above schemes and launder the illegal proceeds by transferring proceeds through multiple bank accounts and thus maintain in the target location the evidence, fruits, and instruments described in Attachment B.


CONCLUSION

13. Based on all the foregoing facts, your affiant believes that there exists probable cause to believe that PELAYO and FREDERICKS, and others known and unknown, are orchestrating schemes to defraud individuals, commit identity theft by use of electronic wires, by laundering the illegal proceeds, and that they maintain evidence of the illegal operation in their residences, vehicles and on their person in violation of Title 18, United States Code, Sections 371, 1343, 1028A, 1956h, and 641.
14. Based upon the foregoing facts and upon Affiant's training and experience, there is probable cause to believe that funds in the Subject Accounts and the Subject Vehicles are: proceeds traceable to violations of Title 18 U.S.C. §§ 371 (Conspiracy to Defraud the United States), 641 (Theft of Public Money), 1343 (Wire Fraud), and 1956(h) (Conspiracy to Commit Money Laundering); subject to civil and criminal forfeiture to the United States pursuant to Title 18

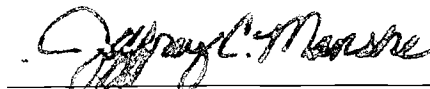
U.S.C. § 981(a)(1)(C) (civil forfeiture), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c); and subject to civil and criminal seizure pursuant to Title 18 U.S.C. § 981(b) (civil seizure) and Title 21 U.S.C. § 853(f) by Title 18 U.S.C. § 982(b)(1) (criminal seizure).

The issuance of the seizure warrants in this district is appropriate under Title 18 U.S.C. § 981(b)(3) and Title 28 U.S.C. § 1355(b)(1) because, notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed.

Further, restraining orders would not be adequate to preserve the properties for forfeiture as the funds in the Subject Accounts and Subject Vehicles can be easily moved, transferred, or dissipated.


RICKY L. WELTON, Special Agent
United States Army
Criminal Investigation Division

SWORN TO AND SUBSCRIBED before me on the 9 day of June, 2020.


JEFFREY C. MANSKE
United States Magistrate Judge

ATTACHMENT A

LOCATIONS TO BE SEARCHED

Your affiant believes that probable cause exists to believe that evidence, fruits, and instrumentalities of the aforementioned violations are maintained at the following locations maintained, used and/or controlled by, PELAYO, FREDERICKS, and/or their close business associates and entities:

- a) 5007 Onion Road, Killeen, Texas, also known as the residence of PELAYO & FREDERICKS.



- b) All outbuildings, garages, and portable sheds located on the property of 5007 Onion Road, Killeen, Texas
- c) Person of Kevin PELAYO
- d) Person of Cristine FREDERICKS

ATTACHMENT B

ITEMS TO BE SEIZED

Any and all evidence, fruits, and instrumentalities of a conspiracy to commit wire fraud, theft of government funds, identity theft, and/or money laundering, including but not limited to, the following:

1. Documents, data, tickets, notices, credit card receipts, travel schedules, travel receipts, passports, and/or records, and other items relating to travel to commit fraud, wire fraud, theft of government funds, identity theft, and money laundering. Evidence of such travel is often times maintained by fraud perpetrators in the form of airline receipts, bus tickets, automobile rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, logs, travel agency vouchers, notes, cellular telephone tolls, and records of long distance telephone calls.
2. Books, mailings, e-mails, text messages, letters, correspondence or communications amongst and between co-conspirators, victims, facilitators, and witnesses related to and in furtherance of the offenses, including but not limited to records, invoices, receipts, records of real estate transactions, financial statements, bank statements, canceled checks, deposit tickets, passbooks, money drafts, withdraw slips, certificates of deposit, letters of credit, loan and mortgage records, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, money wrappers, wire transfer applications and/or receipts, fictitious identification, and other items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money.
3. Electronic equipment, such as currency counting machines, telephone caller identification boxes, cellular telephone(s), smart phones, personal digital assistants (PDAs), and any stored electronic communications contained therein.

4. Contents of the safes, lock boxes, briefcases, and other locked containers located within the residences, vehicles, or on the person of PELAYO, and FREDERICKS which contain evidence of offenses described above.
5. United States currency, money orders, stored value cards, virtual currency or evidence of possession or transfer of virtual currency, precious metals, jewelry, gold coins, vehicles, financial instruments, and other items of value purchased with the fraudulent proceeds including, but not limited to, stocks and bonds.
6. Photographs, including still photos, negatives, video, films, undeveloped film and the contents therein, disks, and slides.
7. Portable electronic devices, such as cell phones, smart phones, and tablet computers to carry-out, store and maintain records in regards to their business activities. Cell phones, smart phones, and tablet computers have evolved to the point that they are in essence miniaturized “computers” unto themselves; capable of performing many of the same functions – and in many cases altogether unique and different functions – as a traditional desktop or laptop computer. These devices allow users to conduct transactions and readily carry-out a variety of tasks from almost anywhere and at any time; and users often keep the devices on or near themselves at all times. These devices can store the same types of records that are stored on desktop and laptop computers, and they are often integrated with and capable of accessing the data and files contained on a user’s home and/or work computer systems. Updates that occur on one device can be accessible and available from any of the devices (computer, laptop, cell phone, smart phone, and/or tablet device, etc.) connected to this network. Even the most basic cell phones typically have the ability to make and receive text messages, take pictures, and/or access the

internet even if only in a rudimentary manner. Users usually maintain these portable electronic devices in their possession, in their vehicles and/or at their residence/business/organization.